DULT Threat Model v01: Updates and Open Issues

Maggie Delano, Swarthmore College
Jessie Lowell, Safety Net Project, NNEDV
Shailesh Prabhu, Nokia

Motivation

- In order for the DULT protocol to be successful, the WG will need an understanding of an unwanted tracking threat model

- DULT Threat Model has been adopted by the WG and includes:
  - A taxonomy of unwanted tracking
  - Methods to Circumvent DULT Protocol (new)
  - What we think should be in/out of scope w.r.t. attackers and victims
  - Design requirements and constraints (new)

- Threat Model v01 has been uploaded

New in v01

- Major changes
  - Added Shailesh Prabhu as author
  - Added Section 3.2: Possible Methods to Circumvent DULT Protocol
  - Added Sections 4.1 Design Requirements and 4.2 Design Constraints
- Minor changes
  - Changed the term “broadcast” to “transmit”
  - Changed definition of tracking tag to “a small device that is not easily discoverable and transmits location data to other devices”
  - Updated tracking taxonomy to include expectation of unwanted tracking

3.2 Possible Methods to Circumvent DULT Protocol

Threat	Impact	Likelihood	Feasibility	Risk Level	Affected Users	Mitigation Available?
Deploying Multiple Tags	High	High	Easy	High	Victims	Partial
Remote Advertisement Monitoring	High	High	Easy	High	All users	No
Non-Compliant Tags	High	Medium	Moderate	Medium	Victims	No
Misuse of Remote Disablement	Medium	Medium	Moderate	Medium	Victims	Partial
Rotating Tracker IDs	High	High	Easy	High	Victims	Partial
Delayed Activation of Trackers	Medium	High	Easy	High	Victims	No
Multi-Tag Correlation Attack	High	Medium	Moderate	Medium	Victims	No
Exploiting Gaps in OS-based Detection	High	High	Moderate	High	All users	Partial
Spoofing Legitimate Devices	Medium	Medium	Moderate	Medium	Victims	No
Heterogeneous Tracker Networks	High	Medium	Hard	Medium	Victims	No

Section 3.2 includes discussion of each of the listed attacks on the DULT Protocol.

Clarifications and additional attacks are being considered in open issues.

4.1 Design Requirements

At the highest level, the DULT protocol should:

1) Allow victims to detect unwanted location tracking
2) Help victims find tags that are tracking them
3) Provide instructions for victims to disable those trackers if they choose

These affordances should be implemented while considering the appropriate privacy and security requirements (currently TODO).

The document goes into more detail about each of these requirements.

4.2 Design Constraints

There are design constraints that the DULT Protocol must consider, including:

1) Bluetooth constraints
2) Power constraints
3) Device constraints

The document goes into more detail about each of these constraints.

All Open Issues

- Additions
  - Attack: nRootTag (#77)
  - Attack: which attacks will we consider out of scope? (#18)
  - **Attack: Tile powered Lenovo Laptops (#78)**
  - Discuss design tradeoffs between privacy of benign tag owners with need for unwanted location tracking (#36, #62)
  - Discuss attacker proximity to victim e.g. access to victim's tracking account (#55)
  - Expand scenarios to incorporate updated taxonomy (#61)
  - **Consider tags paired to multiple accounts/devices (#71)**
- Clarifications / Improvements
  - Update terminology to be consistent with other documents (#33, #34)
  - Clarify what remote disablement entails (#63)
  - Break noncompliant tags into sub section (#64, #69)
  - Clarify remote advertisement monitoring section (#65)
  - Can any attacker who can guess a tag ID query the central server for location? (#66)
  - **Clarify whether we are working with Bluetooth only or other protocols (#67)**
  - Clarify and expand spoofing legitimate devices section (#68)
- Minor additions/fixes
  - Add acknowledgements (#60)
  - Fix duplication of anticipation of unwanted location tracking text (#79)

https://github.com/ietf-wg-dult/threat-model/issues

Attack Tile Powered Lenovo Laptops (#78)

From Jessie: Lenovo is now making laptops that can be activated as Tiles. An abuser could enable the Tile capacity on a survivor's laptop and connect it to abuser's phone without survivor knowing, enabling tracking of where the survivor takes their laptop even if the laptop is turned off.

MD: This is line with other threats with a few differences (using a survivor's own device to track them, instead of their own tag, "tag" is a larger device). Should we require laptops that implement this type of protocol to adhere to the protocol, or should it remain optional? (I'd lean toward requiring if the implementation is very similar)

https://github.com/ietf-wg-dult/threat-model/issues/78

Consider tags paired to multiple accounts/devices (#71)

Brent Ledvina: Eva Galperin in email from 10/18/2024: “I also support adoption, with the caveats that the TODO sections still need to be filled in and that if the behavior of trackers that are paired to multiple devices is outside of the scope of this document, then we need to make sure to cover it somewhere else. Many trackers currently have this capability and I want to make sure that if a person finds an unwanted tracker that they are able to find out about all of the devices that it is paired to, not just the primary one.”

Questions:

- Is this in scope for DULT WG?
  - MD: I say yes. The WG will standardize “actions that these accessories and devices should take once unwanted tracking is detected” and “Develop standards-track guidance for non-owner device platforms necessary to support implementation of the DULT protocol”
- Which document(s) should address this?
  - MD: we can add this to design requirements in our document. There should also be a dedicated section somewhere that provides guidance for non-owner device platforms, which could be in threat model or its own document.

https://github.com/ietf-wg-dult/threat-model/issues/71

Bluetooth vs. other technologies (#67)

“3.1.2. Bluetooth vs. other technologies

The above taxonomy and threat analysis focus on location tracking tags. They are protocol-independent; if a tag were designed using a technology other than Bluetooth, they would still apply. The key attributes are the functionalities and physical properties of the accessory from the user’s perspective. The accessory must be small and not easily discoverable and able to transmit its location to other consumer devices.”

Brent Ledvina: The second sentence in Bluetooth vs other technologies makes a statement that the threat analysis focuses on location tracking tags that use Bluetooth or other technologies. Is this meant to suggest using other technologies than Bluetooth for crowd-sourcing?

Maggie Delano: Clarify to “if a tag were designed for crowd-sourced location tracking using a technology other than Bluetooth?”

https://github.com/ietf-wg-dult/threat-model/issues/67